BANCO DE ESPAÑA
Eurosistema

USO RESTRINGIDO

CIBERSEGURIDAD EN INFRAESTRUCTURAS DEL MERCADO FINANCIERO

María Cristina García Medina

Especialista en sistemas de liquidación de pagos y valores
Unidad de Vigilancia y Análisis de Infraestructuras de Mercado

CURSO SOBRE INFRAESTRUCTURAS DEL MERCADO FINANCIERO

CEMLA - Banco Central de Reserva del Perú - Banco de España

FORMATO VIRTUAL

23 - 27 de noviembre, 2020

SISTEMAS DE PAGO

ÍNDICE

El sector financiero es un objetivo prioritario tanto por motivos económicos como ideológicos

Risk.net
OCC warns on cyber and fraud control lapses during Covid

CENTRAL BANKING
RBNZ warns of cyber risk from cloud
Draft guidelines would mandate firms to notify RBNZ over outsourcing critical functions to cloud

Su fuerte dependencia de las tecnologías de la información lo facilita

Elevada interconexión del sector financiero a nivel nacional e internacional

Risk.net
Cyber attack could freeze US liquidity – NY Fed paper

La innovación financiera y los nuevos participantes han multiplicado los posibles puntos de entrada

BANK OF ENGLAND
18 April 2018

First non-bank payment service provider (PSP) directly accesses UK payment system

Principales características:

- Persistencia y sofisticación
- Múltiples puntos de entrada
- Medidas tradicionales inefectivas
- Sigilo y propagación rápida

Un ataque cibernético puede comprometer:

La importancia de estos ataques dependerá del grado en el que afecten a la actividad de la entidad

Estructura:

- Cinco categorías principales de gestión de riesgos, y
- Tres componentes generales

Claves:

- Enfoque basado en el riesgo
- Todos los elementos son igualmente importantes pero la gobernanza es clave
- No sólo para las IMF
- Importancia de la colaboración

Gobernanza

- **Objetivo**: cultura de ciberseguridad, enfoque proactivo y recursos suficientes.
- Marco de ciberresiliencia y estrategia de ciberseguridad.
- Papel de la alta administración de la IFM y cultura de ciberseguridad.

Identificación

- **Objetivo**: determinar criticidad y priorizar protección.
- Funciones críticas y los activos de información en los que se basan, incluyendo los procesos y procedimientos y sistemas.
- Identificación de interdependencias internas y externas.

Protección

- **Objetivo**: tener controles, sistemas y procesos eficaces y proporcionales a la importancia de la IFM y su riesgo.
- Medidas: para la protección de activos y procesos, interconexiones, amenazas internas, formación.

Detección

- **Objetivo**: tomar contramedidas rápidamente y contener los daños
- Monitorización continua de amplio alcance, medidas de detección a distinto nivel.

Respuesta y recuperación

- **Objetivo**: reinicio de operaciones críticas de forma rápida, segura y utilizando datos fiables. Infraestructuras sistémicas RTO de 2 horas.
- Medidas: planes de respuesta y recuperación, de contingencia, medidas garantizar la integridad de los datos ("replay capability", reconciliación de posiciones), análisis forenses, cooperación.

Pruebas

- **Objetivo**: determinar la efectividad de los controles, procesos y procedimientos implantados o a implantar.
- Medidas: inteligencia de seguridad, análisis de vulnerabilidad, Testing en base a escenarios, pruebas de penetración, Red teaming, incluir al ecosistema.

Concienciación

- **Objetivo**: comprender los ciberriesgos a los que se enfrenta la entidad.
- Medidas: utilización de inteligencia de seguridad, acuerdos para compartir información.

Aprendizaje y evolución

- **Objetivo**: adaptación ante los cambios en las amenazas cibernéticas.
- Medidas: lecciones aprendidas de ataques pasados, formación continua y capacidad de anticipación, utilización de métricas para medir la madurez cibernética de la IMF.

Marzo 2017

1. Preparación de la FMI

Los vigilantes deben trabajar con la FMI para reforzar su ciberresiliencia en un entorno de ciberataques cada vez más sofisticados

3. Diálogo estratégico industria-reguladores

El objetivo es fomentar la cooperación y la confianza, actuar como catalizador de iniciativas para mejorar las capacidades del sector y aumentar la concienciación sobre riesgos cibernéticos y ciberresiliencia

2. Resiliencia del sector

El objetivo es mejorar la resiliencia del sector en su conjunto, impulsando la colaboración transfronteriza y entre autoridades, crear mecanismos para compartir información y el desarrollo de ejercicios de resiliencia del sector

Claves:

- ✓ Enfoque común frente a los riesgos cibernéticos.
- ✓ Sólo IFM competencia del Eurosistema.
- ✓ Participación de países no euro

1. Las expectativas de vigilancia

CROE (*Cyber Resilience Oversight Expectations for FMIs*)

Origen:

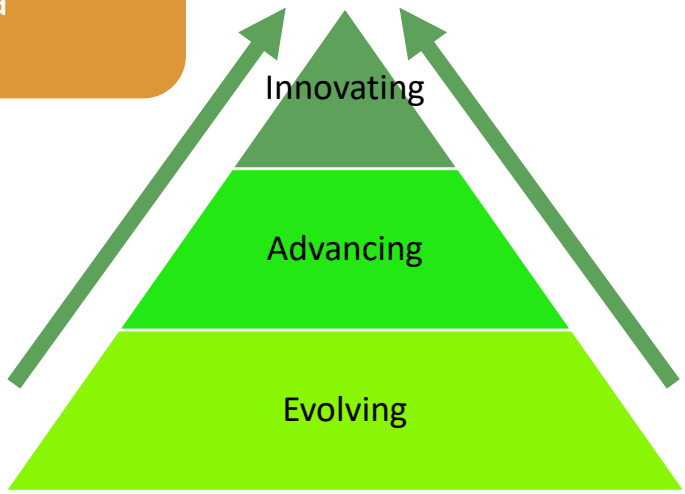
- ✓ Especificación de la Guía de ciberresiliencia de CPMI-IOSCO
- ✓ Recoge estándares y buenas prácticas **existentes** en el mercado

Objetivos:

- ✓ Para el **vigilante**: las expectativas frente a las cuales evalúa a su IMF
- ✓ Para la **IMF**: Puede utilizarse para implantar la guía
- ✓ Para **ambos**: base para la colaboración

Metodología de análisis:

- ✓ Determinación del **nivel de expectativas exigible** a la IMF
- ✓ Aplicación del principio de "**meet or explain**".
- ✓ Principio de **proporcionalidad**



Ejemplo: de la Guía de CPMI-IOSCO a las CROE

Guía CPMI-IOSCO:

6.3.2 Data integrity. In addition, the FMI's cyber resilience framework should include… conducting frequent periodic independent ***reconciliation of participants' positions***

CROE (Cyber Resilience Oversight Expectations for FMIs):

Evolving*: No hay expectativas*

Advancing*: The FMI should conduct* ***frequent periodic reconciliation*** *of participants' positions, with the assistance of participants where needed*

Innovating*: The FMI should consider having a* ***data-sharing agreement*** *with third parties and/or participants in order to obtain uncorrupted data from them for recovering its business operations in a timely manner and with accurate data*

Aplicación práctica de las CROE por el vigilante

Fase 1. Determinación del nivel de expectativas a cumplir por la IMF

- Gobernanza
- Identificación
- Protección
- Detección
- Respuesta y recuperación
- Pruebas
- Concienciación
- Aprendizaje y evolución

Nivel exigido para cada una de las categorías:

- ✓ Evolving
- ✓ Advancing
- ✓ Innovating

Fase 2. Autoevaluación + documentación de soporte. “Meet or explain”.

Fase 3. Informe del vigilante. Hallazgos, recomendaciones e infracciones.

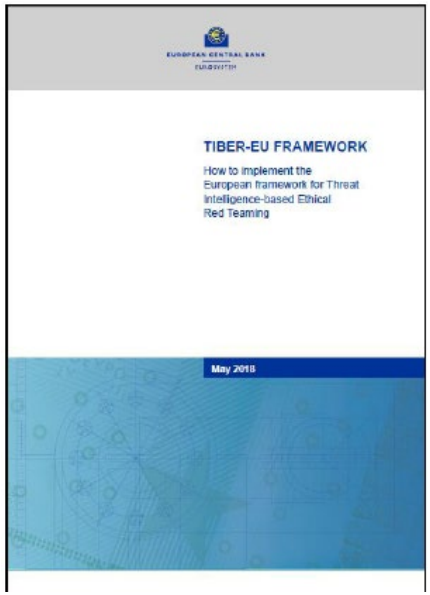
2. El marco TIBER-EU para pruebas de red team

Objetivos

- ✓ Guía para las autoridades
- ✓ Estandarización en la forma de realizar la pruebas
- ✓ Marco común para el reconocimiento de los resultados

Principales características del marco

- ✓ Adopción nacional. Autoridades relevantes.
- ✓ Participación de las entidades: voluntaria u obligatoria
- ✓ Creación del "TIBER-EU Knowledge Centre"
- ✓ Realización por proveedores externos
- ✓ Responsabilidad sobre la prueba y legalidad
- ✓ Organización interna de la prueba



Marco TIBER-EU aprobado por el Consejo de Gobierno en abril de 2018.

Fases:

Informe genérico

- Relativo al sector financiero
- Base para el informe específico de inteligencia de seguridad

Fase preparatoria

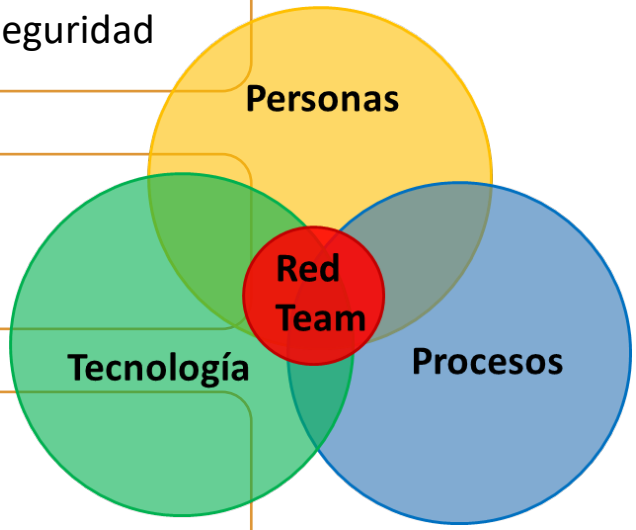
- Lanzamiento formal de la prueba
- Definición del alcance de la prueba
- Selección de los proveedores

Fase de realización

- Informe de inteligencia de seguridad específico
- Realización de la prueba

Fase de cierre

- Informe de vulnerabilidades y recomendaciones
- Plan de mejora en consulta con el vigilante/supervisor



Impacto de los riesgos cibernéticos sobre la actividad de vigilancia de los bancos centrales:

- ✓ No es un riesgo operativo tradicional: cambio de enfoque
- ✓ Iniciativas regulatorias: guía CPMI-IOSCO
- ✓ Estrategia de ciberresiliencia del Eurosistema

Retos:

- ✓ Necesidad de formación más específica y continua. Apoyo del departamento de IT
- ✓ Área muy demandada y más novedosa para los bancos centrales
- ✓ El nivel de exigencia/vigilancia en la práctica puede diferir en gran medida

BANCO DE ESPAÑA
Eurosistema

GRACIAS POR SU ATENCIÓN